Law Firm Announces Recovery Options for Victims of SIM Swapping

NEW YORK, NEW YORK, USA, August 25, 2022 /EINPresswire.com/ -- SIM Swapping, also known as SIM hijacking, results in millions in stolen crypto currency each year. MDF Law is interested in speaking with prospective clients who had more than $250,000 stolen from them because of a SIM swap. If this applies to you or someone you know, please call 800-767-8040 or visit www.mdf-law.com for a free and confidential consultation.


Marc D. Fitapelli, Esq.

What is SIM Swapping?

Recently, sophisticated criminal organizations began targeting people who own large amounts of cryptocurrency. The crime involves convincing (or bribing) a victim's mobile carrier to transfer your SIM information to a hacker's cell phone. Armed with your SIM card, a hacker can take control of your cell phone, change passwords, and steal money, usually in the form of crypto currency. SIM swapping often occurs late at night, over the weekend or during major holidays – all times when you may not immediately notice or care that your cell phone cannot make or receive calls. Virtually every mobile carrier has been impacted by this, including T-Mobile, AT&T and Verizon.

> If your cryptocurrency was stolen as a result of a SIM swap, I may be able to help you recover money."
>
> *Marc D. Fitapelli, Esq.*

How do I know if I was a victim of a SIM swap?

Once the hacker is given access to your SIM, your cell phone stops working, and they begin receiving all your calls and text messages. Hackers can reset your email passwords using your phone number to receive a text message verification from your email provider. This is a common recovery method for lost passwords. Once the hacker has access to your email

account, they can defeat any SMS-based dual factor authentication. They will also search your email account for any other personal information about you they can exploit, including copies of your identification or social security card.

Are victims of SIM hijacking randomly targeted?

No. Hackers already know their victims own large amounts of crypto currency. Victims are identified either through their own negligence or someone else's. For example, you may have been targeted because you fell victim to a phishing scam (your own negligence). Alternatively, your name and crypto balance may have been leaked as part of a data breach (someone else's negligence). You may still have a claim even if you were targeted due to your own negligence. Each situation is unique, and you should speak with an attorney to determine your legal rights.

What should I do if I was a victim of a SIM swap?

Immediately report the crime to your local police or the FBI. You must also immediately contact your mobile provider as well as any financial institution that holds money or cryptocurrency on your behalf. Lastly, once you have access, change all your passwords and establish a new method for dual factor authentication (see below).

What could I do to protect myself from a SIM swap?

You should always use dual factor authentication for all of your accounts. However, you should avoid using SMS text messages for dual factor authentication. Instead, use dual factor authentication apps or a physical security key. Using a physical security key is the most prudent measure you can currently take according to the FBI.

What laws apply to mobile carriers?

Mobile carriers are required under federal law to safeguard customer information. The Federal Communications Act of 1934 and the regulations implemented thereafter by the FCC serve as a basis for their liability. Under those regulations, mobile carriers are obligated to take specific steps to protect their customer's personal information. Most cell phone providers have histories of fines related to their violation of these regulations.

Can I sue my mobile carrier in court?

Probably not. You likely must arbitrate your case based on the terms of your customer account agreement. Most mobile carriers require arbitration before the American Arbitration Association, or AAA.

Could I sue the crypto exchange that facilitated the transfer?

Yes. Crypto exchanges that negligently facilitate this type of activity could be liable to their customers for significant money damages. The most popular centralized exchanges, including Coinbase and Gemeni, are required to comply with the Bank Secrecy Act as well as the U.S. Patriot Act. Under these laws, exchanges are required to implement anti-money laundering (AML) procedures as well as other safeguards to detect and prevent criminal activity.

Is it possible to pursue the criminal who stole my crypto?

Yes, but recovery is unlikely in most situations. The chances of recovering are also directly related to how quickly you respond. The quicker the response the more likely someone (your attorney, exchange or law enforcement) can recover assets from the wrong doer. No matter how quickly you respond, it may not be possible to recover the stolen funds directly from the criminal if the money has already been moved to cold storage or the dark web.

More about MDF Law

MDF Law is a New York city based law firm that represents investors. It is owned by attorney Marc D. Fitapelli. Over his career, Mr. Fitapelli has helped investors recover over $100 million from banks, broker-dealers and other major financial institutions. In addition to being a licensed attorney, Mr. Fitapelli is also a CCI, or Certified Cryptocurrency Investigator. If you have any questions about SIM swaps, including legal options for victims, please call Mr. Fitapelli or his partner, Jeffrey Saxon, at 800-767-8040.

This press release is ATTORNEY ADVERTISING and prior results do not guarantee a similar outcome. Your personal situation may involve unique legal and factual issues. If you were a victim of a SIM swap, contact an attorney immediately to learn your rights.

MDF Law is located at 28 Liberty Street, 30th Floor, New York, New York 10005.

Marc Fitapelli
MDF Law
+1 212-658-1501
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/587752021

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2022 Newsmatics Inc. All Right Reserved.